I claim:

Sub A5 7

1. A method for identifying presence of malicious code in program code within a computer system, the method comprising:

initializing a virtual machine within the computer system, the virtual machine comprising software simulating functionality of a central processing unit and memory;

virtually executing a target program within the virtual machine so that the target program interacts with the computer system only through the virtual machine;

analyzing behavior of the target program following virtual execution to identify occurrence of malicious code behavior and indicating in a behavior pattern the occurrence of malicious code behavior; and

terminating the virtual machine after the analyzing process, thereby removing from the computer system a copy of the target program that was contained within the virtual machine.

2. The method of claim 1, wherein the virtual machine simulates functionality of input/output ports, operating system data areas, and an operating system application program interface.

3. The method of claim 2, wherein the virtual machine further includes a virtual Visual Basic engine.

Sub A5

4. The method of claim 2, wherein virtual execution of the target program causes the target program to interact with the simulated operating system application program interface.

5. The method of claim 1, wherein the target program is newly introduced to the computer system and not executed prior to virtually executing the target program.

6. The method of claim 1, wherein after a first instance of a first program is analyzed by the virtual machine and a first behavior pattern is generated and stored in a database within the computer system, the method further comprising:

determining that the first program is modified;

analyzing the modified first program by executing the modified first program in the virtual machine to provide a second behavior pattern; and

comparing the first behavior pattern to the second behavior pattern.

7. The method of claim 6, wherein a new behavior pattern is generated each time the first program is modified.

Sub A5 7

8. The method of claim 6, wherein introduction of malignant code during modification of the first program is detected by comparing the first behavior pattern to the second behavior pattern.

9. The method of claim 6, wherein the first behavior pattern is substantially similar to the second behavior pattern when the modified first program is a new version of the first program.

10. The method of claim 1, wherein the behavior pattern identifies functions executed in the virtual execution of the target program, the method further comprising tracking an order in which the functions are virtually executed by the target program within the virtual machine.

Sub A5

11. A method for identifying presence of malicious code in program code within a computer system, the method comprising:

initializing a virtual machine within the computer system, the virtual machine comprising software simulating functionality of a central processing unit, memory and an operating system including interrupt calls to the virtual operating system;

virtually executing a target program within the virtual machine so that the target program interacts with the virtual operating system and the virtual central processing unit through the virtual machine;

monitoring behavior of the target program during virtual execution to identify presence of malicious code and indicating in a behavior pattern the occurrence of malicious code behavior; and

terminating the virtual machine, leaving behind a record of the behavior pattern characteristic of the analyzed target program.

12. The method of claim 11, wherein the record is in a behavior register in the computer system.

Sub A5

13. The method of claim 11, wherein after a first instance of a first program is analyzed by the virtual machine and a first behavior pattern is generated and stored in a database within the computer system, the method further comprising:

determining that the first program is modified;

analyzing the modified first program by executing the modified first program in the virtual machine to provide a second behavior pattern; and

comparing the first behavior pattern to the second behavior pattern.

14. The method of claim 13, wherein a new behavior pattern is generated each time the first program is modified.

15. The method of claim 13, wherein introduction of malignant code during modification of the first program is detected by comparing the first behavior pattern to the second behavior pattern.

16. The method of claim 13, wherein the first behavior pattern is substantially similar to the second behavior pattern when the modified first program is a new version of the first program.

Sub A57

17. The method of claim 13, wherein the behavior pattern identifies functions executed in the virtual execution of the target program, the method further comprising tracking an order in which the functions are virtually executed by the target program within the virtual machine.

Add A67